SECURE WIRELESS BACKUP MECHANISM

Inventors: Mika Leppinen, Padma Sachin and Anil Y. Reddy

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to wireless systems and secure backup. More particularly, the present invention relates to a method and system for securely storing data in a public storage area over a wireless network.

2. Description of the Related Art

Mobile client devices, such as mobile telephone handsets, personal digital assistants (PDAs) and wireless computing devices, will have an ever increasing role in the future for accessing and securely storing sensitive data, whether personal or system data, in a public storage area over a wireless network.

Figure 1 shows a functional block diagram of a wireless terminal 100 that provides a conventional secure backup over a wireless network. Wireless terminal 100 includes a memory 101 for storing data and a backup/restore module 102. In the situation when data, such as personal data and/or system data, is to be encrypted by a user, the user specifies data that is to be encrypted and then supplies the user's public encryption key to backup/restore module 102. Backup/restore module 102 accesses the specified data in memory 101 and encrypts the specified data using the user's public key. The encrypted data is sent to, for example, a public storage area 103 over a wireless network 104 in a well-known manner. The encrypted data can only be decrypted using the user's private key. When the user desires to access the stored encrypted data, the encrypted data is downloaded from storage area 103 and decrypted by backup/restore module 102 using the user's private key in a well-known manner.

Nevertheless, what is needed is a convenient way for securely storing sensitive data in a public storage area over a wireless network. Additionally, what is needed is a way to conveniently share sensitive data among different users.

SUMMARY OF THE INVENTION

The present invention provides a convenient way for securely storing sensitive data in a public storage area over a wireless network. The present invention also provides a way to conveniently share sensitive data among different users. In that regard, the present invention provides a technique for securely backing-up data over a wireless network and then later retrieving the securely backed-up data. The data that is to be backed up is encrypted using a public key of the user and is sent over the wireless network, preferably contained within the body of a synchronization message, such as a SyncML document or an XML document. The encrypted data can be later retrieved and decrypted using the private key of the user. Privacy of the encrypted data is protected as long as the private key of the user has not been compromised.

The advantages of the present invention are provided by a method and a system for backing-up data in a wireless network. According to the invention, data is selected within a wireless device, such as a wireless telephone handset or a personal digital assistant, for backup in a storage area that is accessible by the wireless device through the wireless network. The selected data is encrypted using a private key, and then sent to the public storage area preferably using a Wireless Application Protocol (WAP) technique and preferably encapsulated within a SyncML document or an XML document. The encrypted data can later be downloaded from the public storage area preferably using a WAP technique, and the encrypted data is decrypted using a private key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the accompanying figures in which like reference numerals indicate similar elements and in which:

Figure 1 shows a functional block diagram of a wireless terminal that provides secure backup over a wireless network;

Figure 2 shows a functional block diagram of a wireless terminal that provides secure backup over a wireless network according to the present invention; and

Figure 3 shows a flow diagram 300 for backing-up data in a wireless network according to the present invention.

DETAILED DESCRIPTION

The present invention provides a technique for securely storing sensitive data in a public storage area from a client wireless terminal over a wireless network. The data that is to be backed up is encrypted using a public key and is sent over the wireless network using a Wireless Application Protocol (WAP) technique and preferably contained within the body of a SyncML document or an XML document. The encrypted data can be later retrieved and decrypted using the private key of the user.

Figure 2 shows a functional block diagram of a wireless terminal or computing device 200, such as a wireless handset or a personal digital assistant (PDA), that provides secure backup over a wireless network according to the present invention. Wireless terminal 200 includes a native application 201, a backup/restore module 202, a backup application 203 and a Wireless Application Protocol (WAP) browser 204. According to one

variation of the invention, wireless terminal 200 operates as a WAP client device and uses a Wireless Identity Module (WIM) 205 that is preferably tamper-resistant so that the keys, the certificate and the certification standard that are stored within WIM are not easily compromised.

When a user desires to store data within native application 201, such as personal data and/or system data, in a public storage area 206, the user can select the desired data through WAP browser 204 by interacting with backup application 203. Native application 201 then sends the desired data for encryption and backup to backup/restore module 202. WIM 205 provides the user's public key to backup/restore module 202 for encrypting the selected data using, for example, a conventional public key encryption algorithm. The encrypted data is then sent to public storage area 206 through a WAP gateway 207. That is, wireless terminal 200 encapsulates the encrypted data in the body of a SyncML document or XML document and sends the encapsulated, encrypted data to WAP gateway 207 through backup application 203 using the WAP protocol. WAP gateway 207 forwards the encapsulated encrypted data to public storage area 206 using, for example, the HTTP protocol. The particular public storage area selected by the user is specified by the user and is contained in user configuration data or operator setup data within wireless terminal 200.

Encrypted data that is stored in public storage area 206 can be accessed by using WAP browser 204 through backup application 203, and is preferably identified by a Uniform Resource Identifier (URI). To restore encrypted data, WAP browser 204 downloads the desired encrypted data using the WAP protocol and sends the downloaded data to backup/restore module 202 for decryption. The user's private key is supplied to backup/restore module 202 by WIM 205. Once decrypted, the data is sent to native application 201 for restoration.

WIM 205 allows that a user can securely store data from one wireless terminal device and securely access the stored data from another wireless terminal device. That is, WIM 205 stores the certification standard, and the keys and the certificate that are unique to a particular user. Thus, a user can encrypt sensitive data on one wireless terminal device for storage in a public storage area using the user's WIM. The user can then access the encrypted data stored in the public storage area from another wireless terminal device as long as the user uses the same WIM.

Figure 3 shows a flow diagram 300 for backing-up data in a wireless network according to the present invention. At step 301, a user selects data within a wireless client device for backup in a public storage area that is accessible by the wireless client device through the wireless network. At step 302, the selected data is encrypted using a public key for the user supplied by a WIM associated with the user. At step 303, the encrypted data is preferably encapsulated within a SyncML document or an XML document. At step 304, the encrypted data is sent to the public storage area using a WAP technique. Later, at step 305, the user accesses and downloads the encrypted data in the public storage area using WAP technique. At step 306, the downloaded encrypted data is decrypted using a private key of the user that is supplied by the WIM associated with the user.

While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.